



#2182  
RECEIVED

MAY 17 2002

Technology Center 2100

- 071308.0250  
PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Büssert  
Serial No. : 10/056,905 Examiner: To Be Assigned  
Filed : November 13, 2001 Group Art Unit: 2182  
For : ENCRYPTION OF CONTROL PROGRAMS

SUBMISSION OF PRIORITY DOCUMENTS

I hereby certify that this paper is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on:

March 25, 2002  
Date of Deposit

Signature

Bradley B. Geist  
Attorney Name

27,551  
Registration No.

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

We enclose herewith the German patent application nos. 10064400.7, 10063059.6, 10062741.2, 10125383.4, 10125386.9 and 10138533.1, which are the priority documents for the above referenced patent application.

Respectfully submitted,

Bradley B. Geist  
Patent Office Reg. No. 27, 551  
Attorneys for Applicant  
(212) 408-2562

Enclosures



**RECEIVED**  
MAY 17 2002  
Technology Center 2100

**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**Aktenzeichen:** 100 63 059.6

**Anmeldetag:** 18. Dezember 2000

**Anmelder/Inhaber:** Siemens AG, München/DE

**Bezeichnung:** Schutz von Textdaten und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln

**IPC:** G 06 F 12/14

**Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.**

München, den 7. November 2001  
**Deutsches Patent- und Markenamt**  
**Der Präsident**

Im Auftrag

Sieck

## Beschreibung

Schutz von Textdaten und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln

5

Im Zuge der Verbreitung von XML als Speicherformat für Daten geht die Möglichkeit, Daten und Programme gegen Analyse und Benutzung durch Unbefugte zu schützen verloren.

10 Das Problem ist neu und wurde bisher nicht gelöst.

Durch die Integration einer Entschlüsselung in einen Preprozessor unter Verwendung von asymmetrischen Schlüsseln (siehe PGP) ergeben sich folgende Vorteile:

15

a) Die bekannten Routinen für Ver- und Entschlüsselung wandelt von ASCII-Text in ASCII-Text. Die verschlüsselten Bereiche lassen sich also genauso speichern und transportieren wie die unverschlüsselten Bereiche und bieten damit eine ideale Integration in XML.

20

b) Durch das Textformat lassen sich auch Teile eines Textes verschlüsseln. Man kann also den Kopf eines Programmes mit Defines zum Anpassen unverschlüsselt lassen, den Körper mit den Funktionen aber schützen.

25

c) Der Lieferant einer Anwendersoftware (z.B. Compiler oder Projektiertool) gibt dieser ein eigenes Schlüsselpaar. Der Lieferant speichert den Public Key mit den Kundendaten des Anwenders. Jetzt kann der Lieferant Bibliotheken für bestimmte Kunden mit deren Public Key verschlüsseln und über beliebige Kanäle an diese Kunden übermitteln. Jegliche Kopie ist sinnlos, da die Bibliothek ausschließlich auf der Anwendung des vorgesehenen Kunden entschlüsselt werden kann. Ein Lizenzsystem ist damit leicht realisierbar.

30

35 d) Die verschlüsselten Texte sind nicht analysierbar. Ein Know How Diebstahl ist nicht möglich.

Die Kombinierung der an sich bekannten Verfahren ist neu.

Für die Realisierung des Verfahrens wird im Engineering System ein Export- und ein Import-Mechanismus für Projektierdaten im XML-Format verwendet. Damit werden Probleme bei Versionsübergängen, Dokumentation und Analyse gelöst.  
5 Eine Bibliothek auf Basis der exportierten XML-Daten bringt weitere Vorteile.

Durch die Integration einer asymmetrischen Entschlüsselung in  
10 einen Preprozessor des Compilers lassen sich Programmteile gegen Missbrauch schützen, ohne den Compiler selber zu ändern. Der Preprozessor läuft nur bei der Erzeugung des binären Codes für das Zielsystem. Der Programmeditor benötigt auch keine Änderung. Es wird nur der Verschlüsselte Text an-  
15 gezeigt.

Eine Integration einer asymmetrischen Verschlüsselung als Postprozessor in den Export der Parameter ermöglicht auch den Schutz der projektierten Daten. Der Import erhält dann ebenfalls einen Preprozessor für die Parameter.

20

Probleme bei der Vermarktung von werden durch das erfindungsgemäße Verfahren und den erfindungsgemäßen Mechanismus gelöst. Mit der bisherigen Technik ist ein Know How Schutz nicht möglich. Jeder kann die XML-Daten lesen und die enthaltene Parametrierung und Programme lesen, kopieren und für eigene Zwecke einsetzen.  
25

## Patentansprüche

1. Verfahren zur Verschlüsselung und Entschlüsselung von  
Textdaten und Programmen, unter Verwendung eines Public  
5 Key,

gekennzeichnet durch eine Untermenge folgender Merkmale:

- Beschreibung der Daten und Programme in XML,
- Verwendung von asymmetrischen Schlüsseln
- Verschlüsselung und/oder Entschlüsselung durch einen Pre-  
10 Processor
- Gleichbehandlung von verschlüsselten und unverschlüsselten  
Bereichen bei der Speicherung.

2. System zur Verschlüsselung und Entschlüsselung von Textda-  
15 ten und Programmen, unter Verwendung eines Public Key,

gekennzeichnet durch eine Untermenge folgender Merkmale:

- Beschreibung der Daten und Programme in XML,
- Verwendung von asymmetrischen Schlüsseln
- Verschlüsselung und/oder Entschlüsselung durch einen Pre-  
20 Processor
- Gleichbehandlung von verschlüsselten und unverschlüsselten  
Bereichen bei der Speicherung.

Anhang zur Erfindungsmeldung:  
Schutz von Textdateien und Programmen gegen unbefugte Analyse und Benutzung unter Verwendung von asymmetrischen Schlüsseln

